Attributes for NexGen Space Transportation

Wilson Harkins
Deputy Chief Safety and Mission Assurance
NASA Headquarters
Office of Safety and Mission Assurance

Human Space Flight Current Approach

- Human Rating
- Oversight/Insight
- Safety Focus

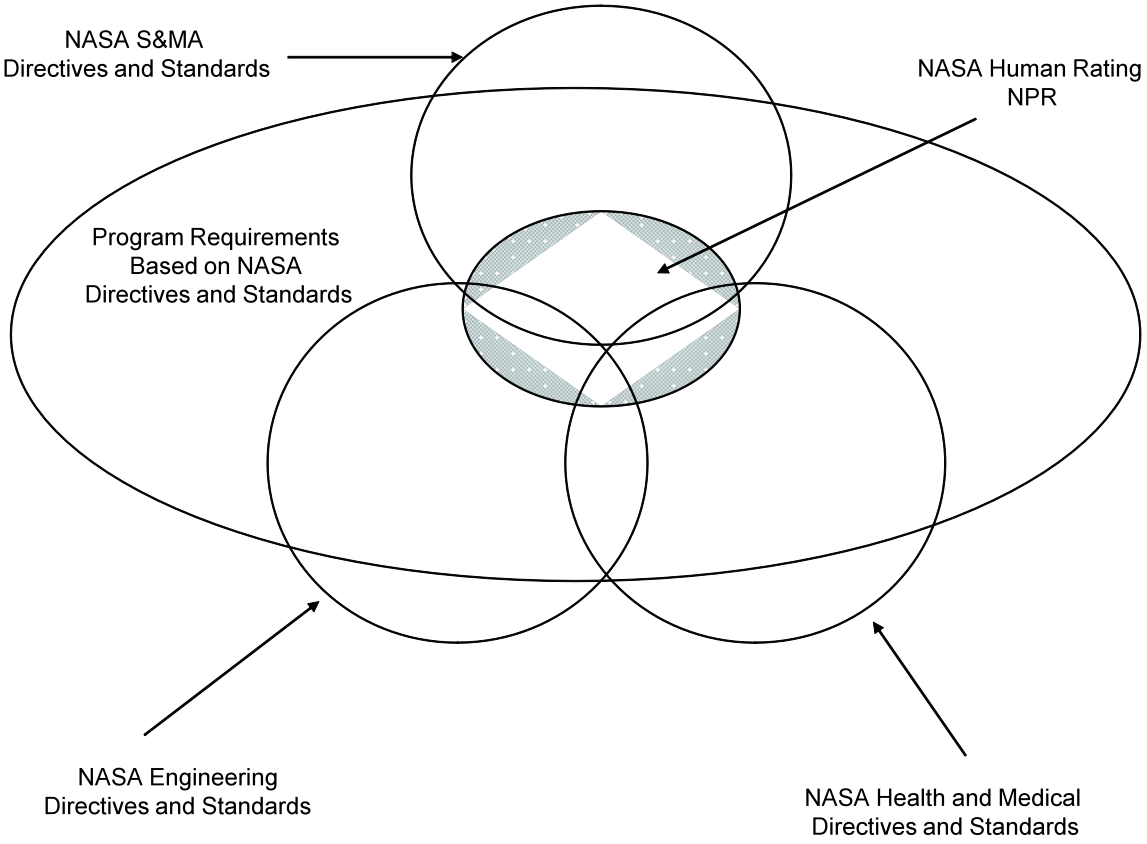
Human Rating Lessons Learned

- Challenge the Design
  - Apollo had an independent set of experts that were important to make us think about what we were doing
  - We insisted that we must have a strong engineering and safety organization that challenges the program on a daily basis.
  - No one used to have to come and challenge the program. The system challenged.
- Understand the Design
  - Don’t want requirements to be a crutch - redundant inspections don’t work - people will use them to defend what they did rather than think through the right thing to do
  - After you get through with the design, you (manager) want the designer to tell you what he couldn’t do, so you know where the weaknesses are and that we both can agree what is the right approach

Human Rating Lessons Learned

- **Incorporate the Human into Design**
  - **Fundamental difference between the philosophy the Russian's used for design than we used. We did everything we could to design the humans in where the Russians went with an automatic system with human watching. Want to design the human in where they can improve the reliability of the system.**
- **Responsibility**
  - **Can't design by committee, someone has to feel responsible.**

Human Rating Concept



Human Rating Concept

- ***Human-rating consists of three fundamental tenets:***
  - ***(1) Human-rating is the process of designing, evaluating, and assuring that the total system can safely conduct the required human missions.***
  - ***(2) Human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success.***
  - ***(3) Human-rating includes the incorporation of design features and capabilities to enable safe recovery of the crew from hazardous situations.***
- ***Human-rating is an integral part of all program activities throughout the life cycle of the system, including design and development; test and verification; program management and control; flight readiness certification; mission operations; sustaining engineering; maintenance/upgrades; and disposal.***

Human Rating Sample Requirements

- 2.3.3 Documenting the Design Philosophy for Utilization of the Crew. At SRR, the Program Manager shall document, in the HRCP, a description of the design philosophy which will be followed to develop a system that utilizes the crew's capabilities to execute the reference missions, prevent aborts, and prevent catastrophic events
- 2.3.7.1 The Program Manager shall perform an integrated safety and design analysis to determine the following:
  - a. The requirements for additional levels of failure tolerance (above the minimum of 1 failure tolerant per 3.2.2) for the space system.
  - b. The appropriate implementation of failure tolerance for the space system, to include an evaluation of dissimilar redundancy and backup systems

Human Rating Sample Requirements

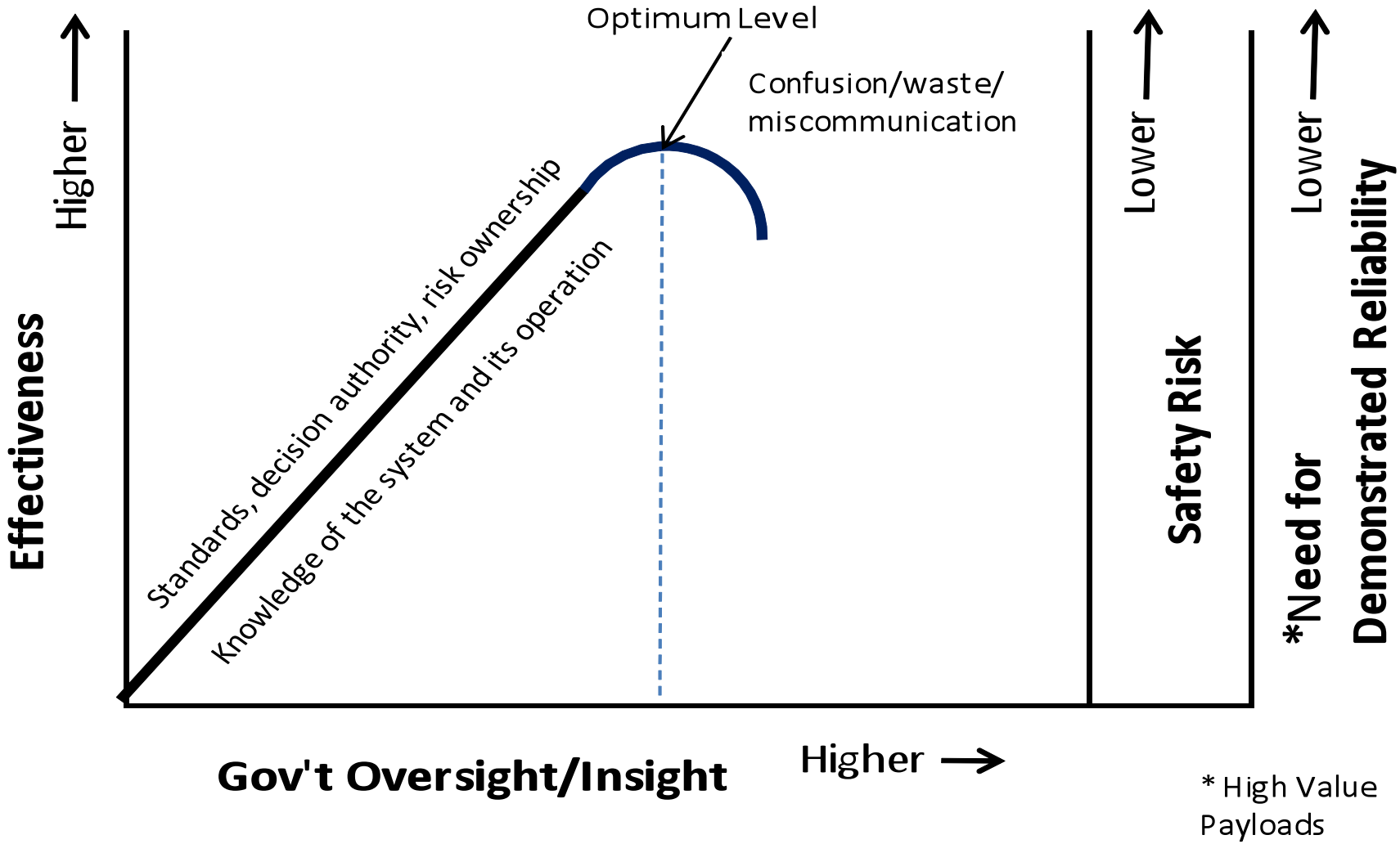
- **3.6.1.2 The space system shall provide abort capability from the launch pad until Earth-orbit insertion to protect for the following ascent failure scenarios (minimum list):**
  - **a. Complete loss of ascent thrust/propulsion**
  - **b. Loss of attitude or flight path control**
- ***Coming Attractions – Loss of Crew Number***

Oversight/Insight

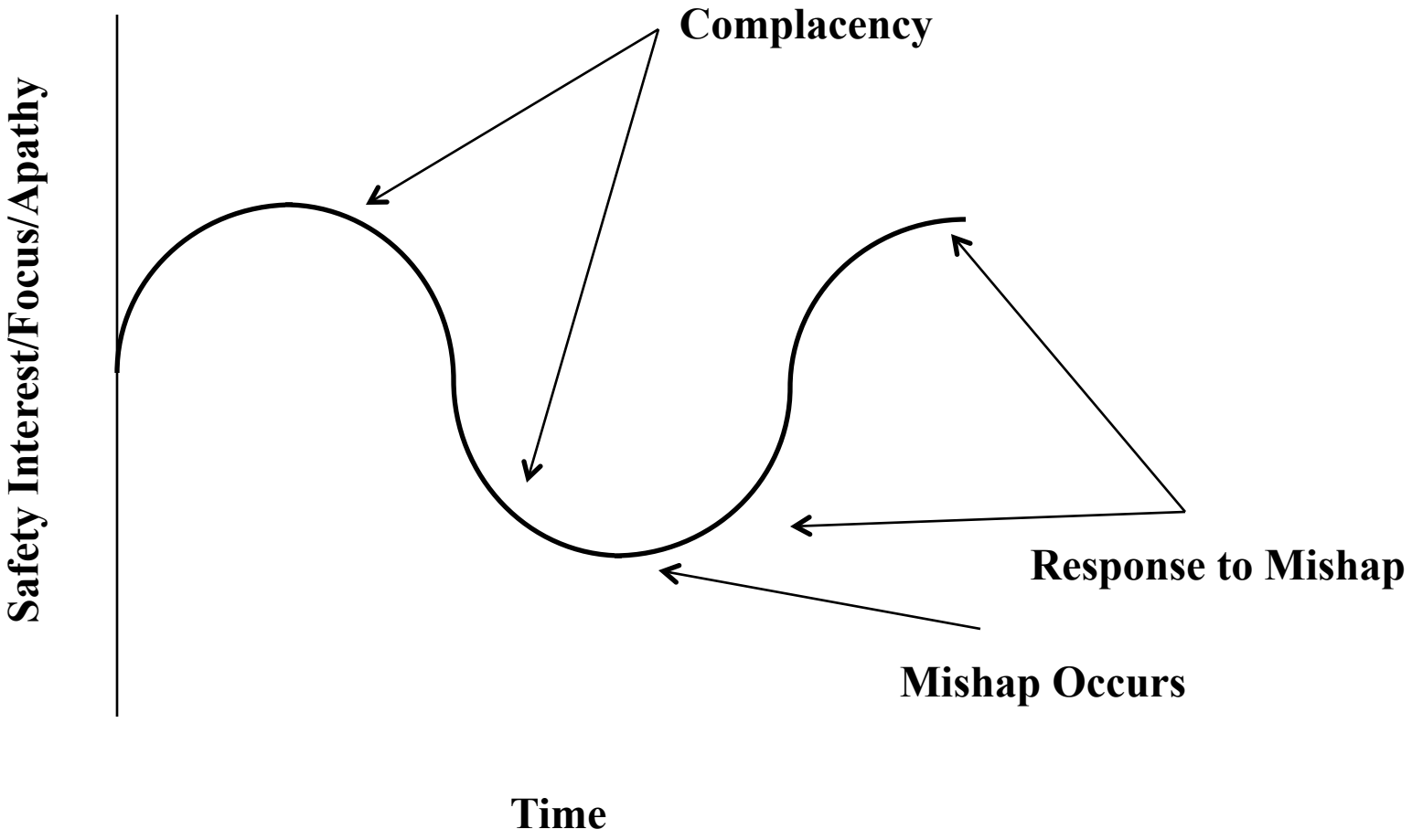
- “Surveillance may be conducted through "insight" or “oversight.” Insight requires the monitoring of Government-identified metrics and contracted milestones. Insight is a continuum that can range from low intensity, such as reviewing quarterly reports, to high intensity, such as performing surveys and reviews. Oversight occurs in line with the contractor's processes. The Government retains and exercises the right to concur or nonconcur with the contractor’s decisions. Nonconcurrence must be resolved before the contractor can proceed. Oversight is a continuum that can range from low intensity, such as Government concurrence in reviews (e.g., PDR, CDR), to high intensity oversight, in which the Government has day-to-day involvement in the contractor’s decision making process (e.g., hardware inspections). “ NFS 1846
- Oversight – Owning Risk – Control
- Insight - Knowledge

Oversight and Insight Effectiveness

(Notional)



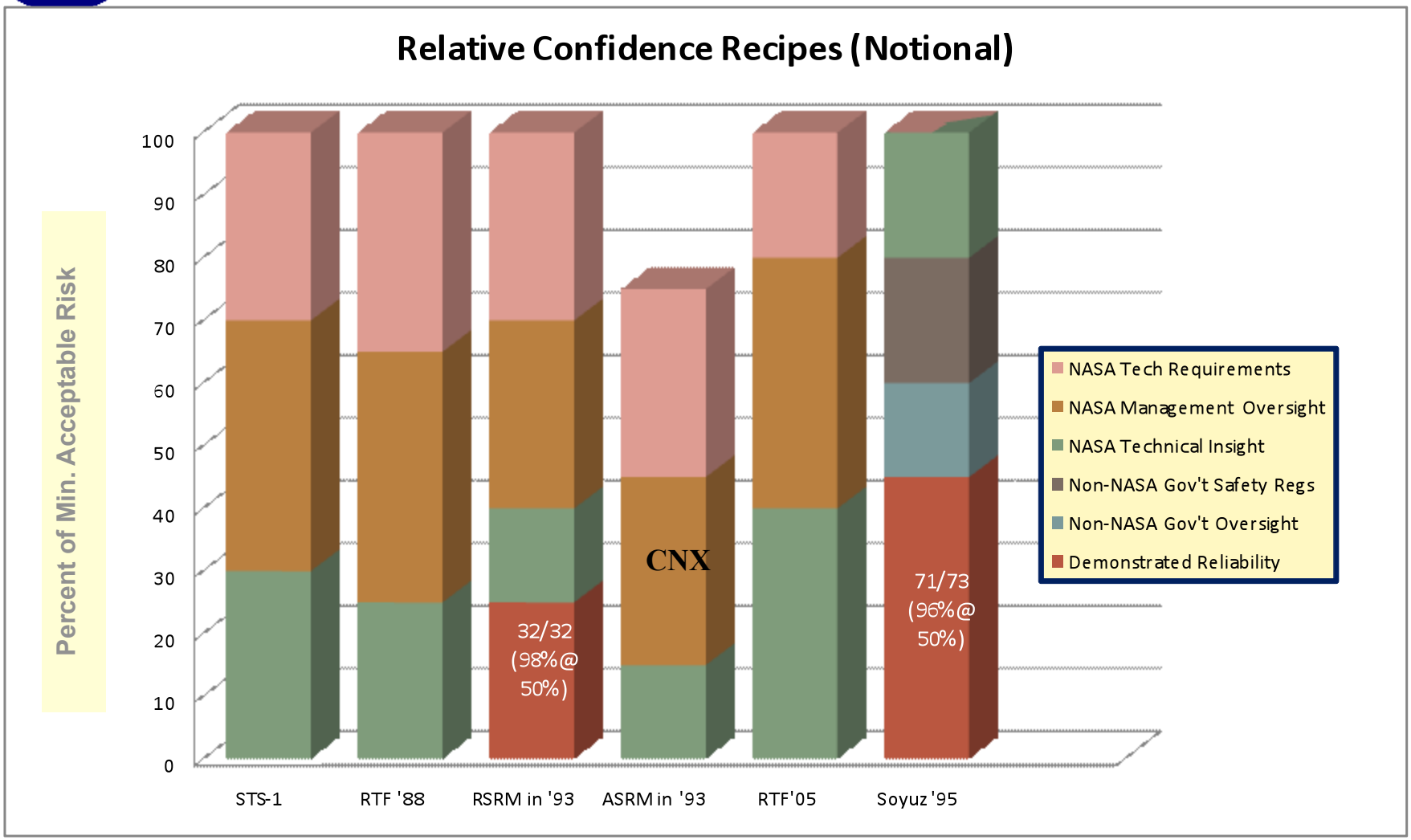
Breaking the Sine Curve



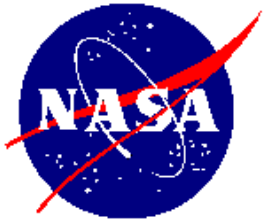
Nex Gen – "Human Rating"

- NPR 8705.2 Human Rating Requirements was written based upon a NASA managed program model
  - Commercial in the same sense that Shuttle was a commercial activity
  - Not required to be applied to other acquisition models
- NPR 8715.3 General Safety Program Requirements includes section 1.14 Hazardous Work Activities that are Outside NASA Control
  - Applies to commercial human space flight where current federal requirements do not necessarily provide for safety of space vehicle occupants
  - Document and verify that risks are adequately controlled and any residual risk is acceptable
  - Review team evaluates system and recommends acceptance

What Gives Us Confidence to Fly People?

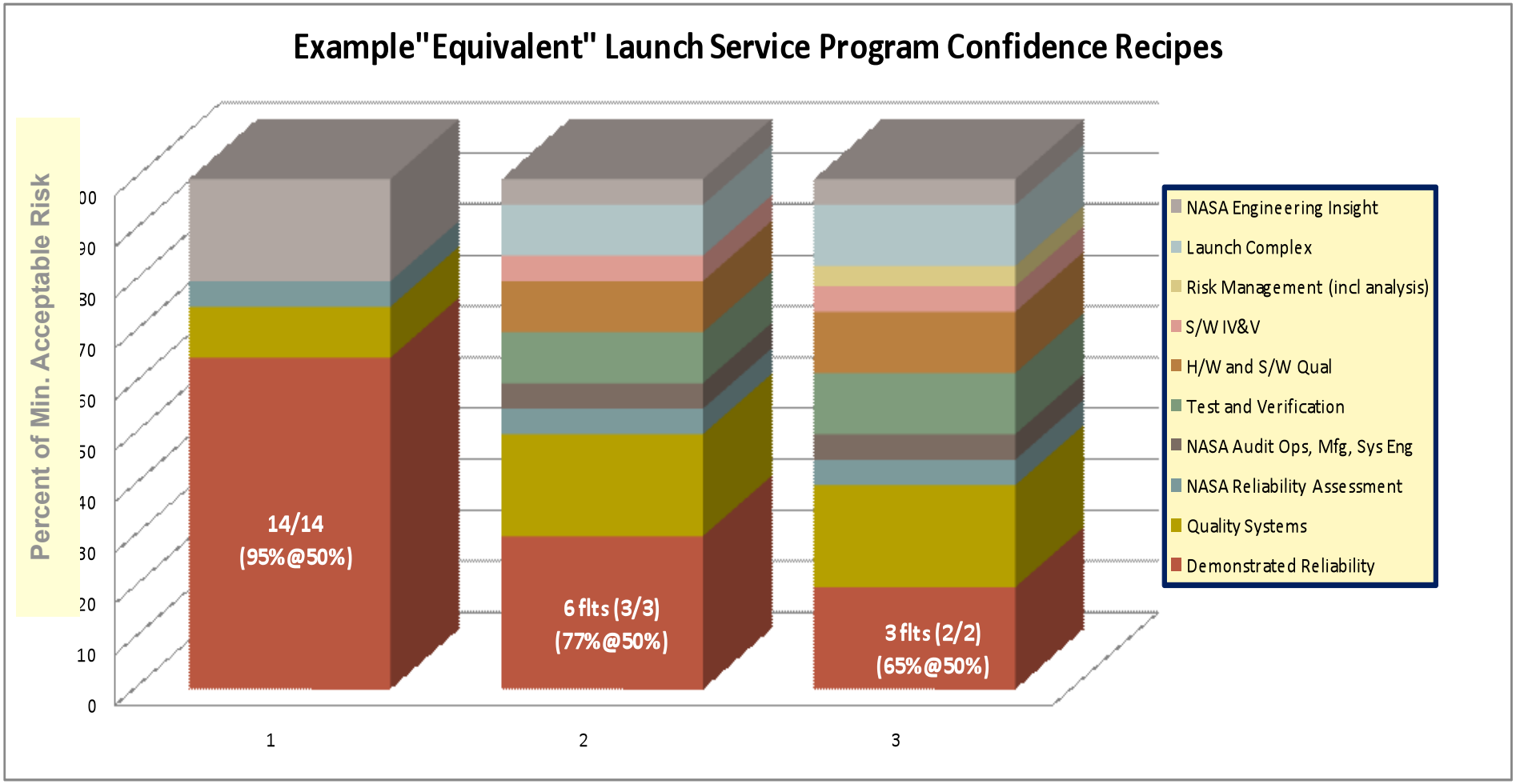


- **The key for NexGen Systems will be to establish the “best recipe” of the ingredients necessary to document and verify that risks are adequately controlled and any residual risk is acceptable while avoiding ending up on the wrong side of the sine curve.**

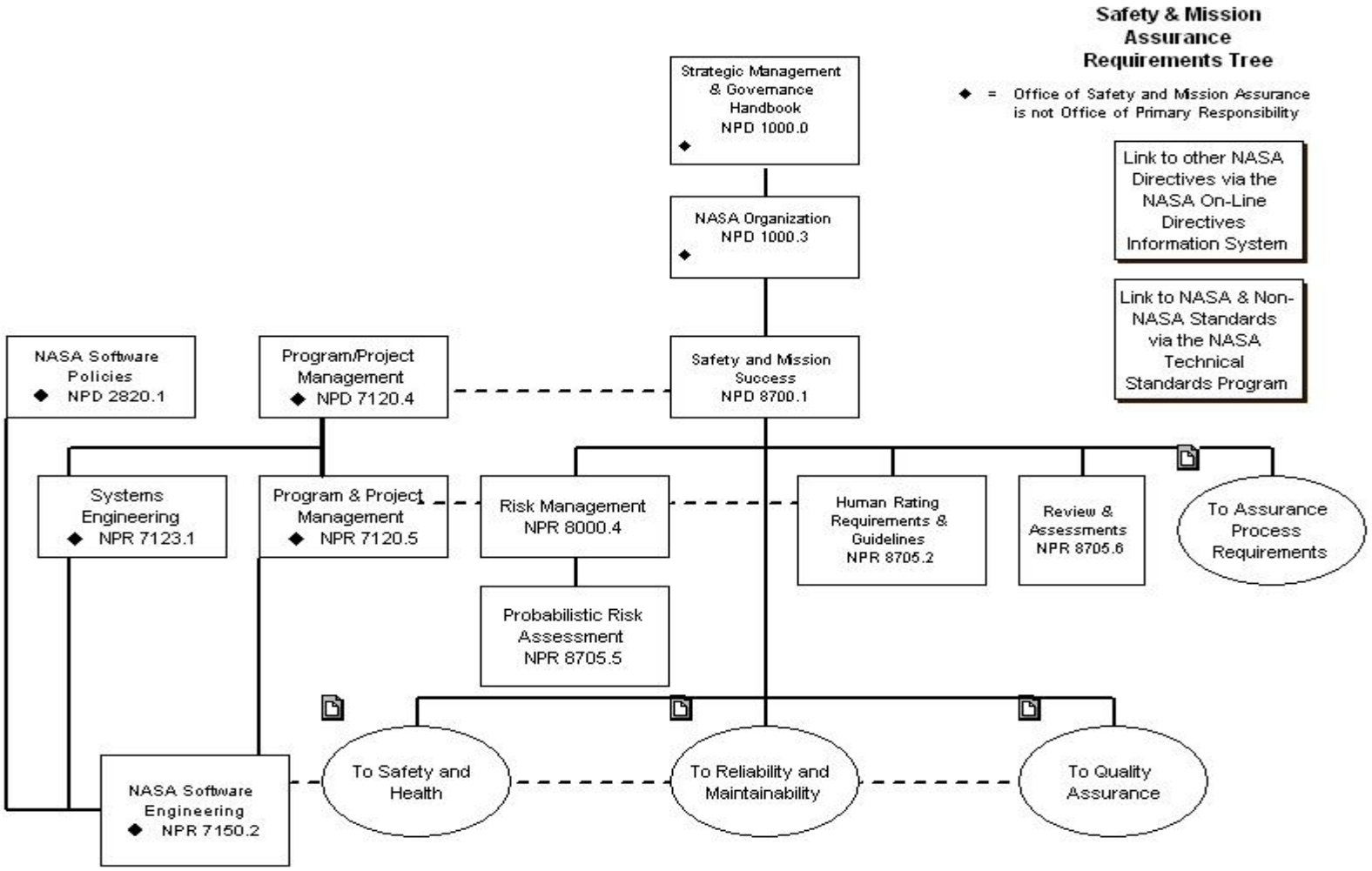


Backup

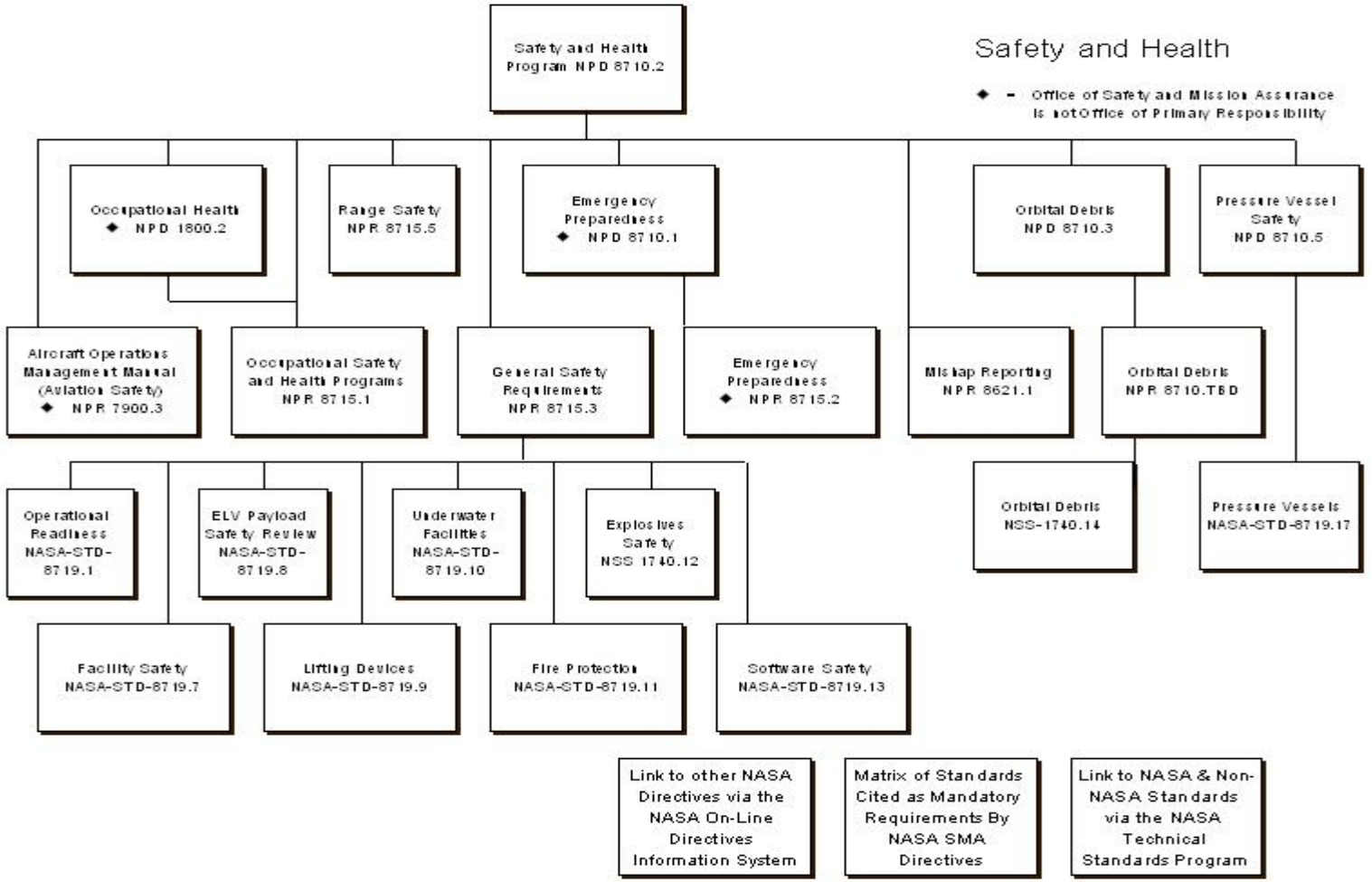
What Gives Us Confidence to Fly Payloads?



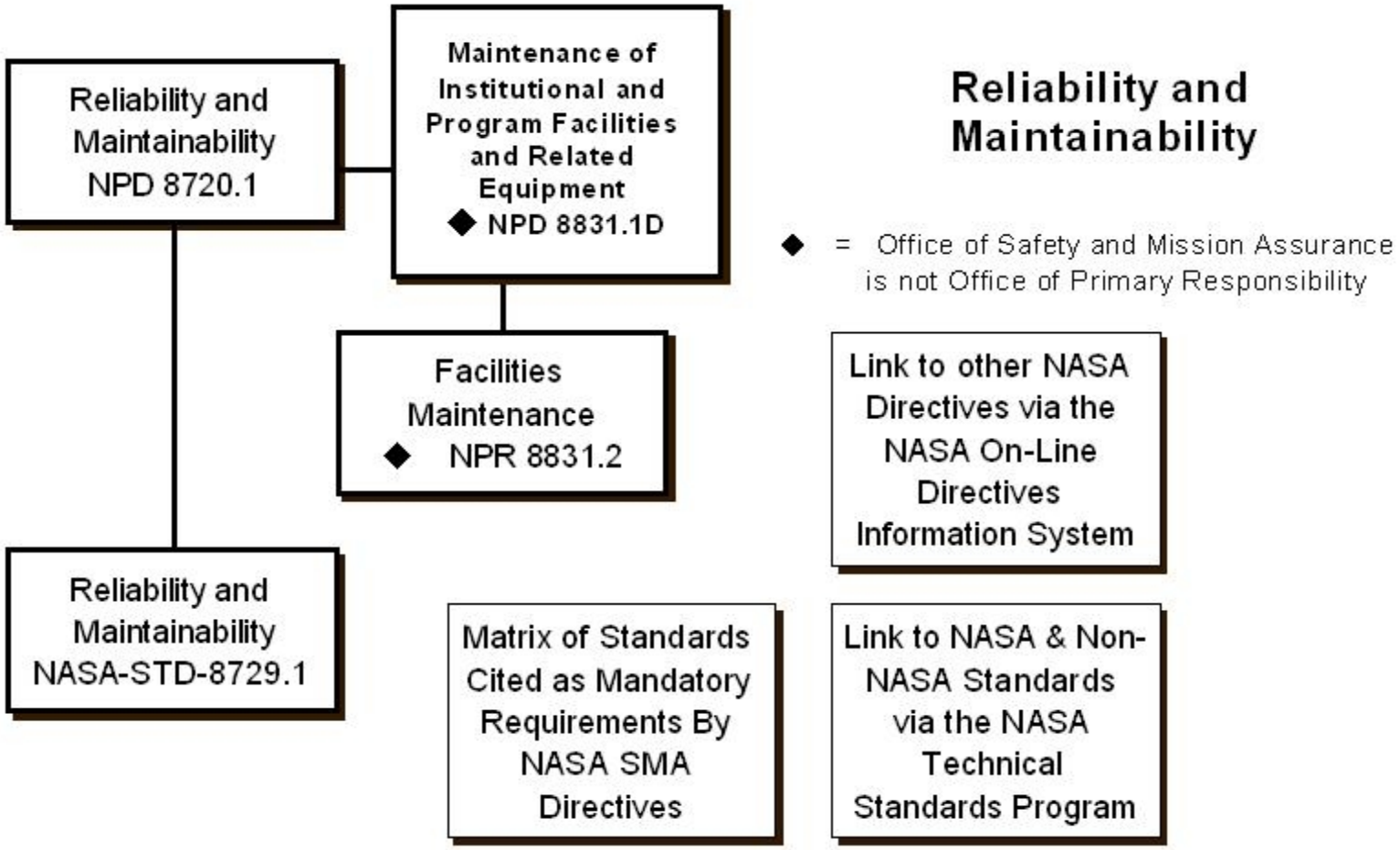
Safety and Mission Assurance Requirements



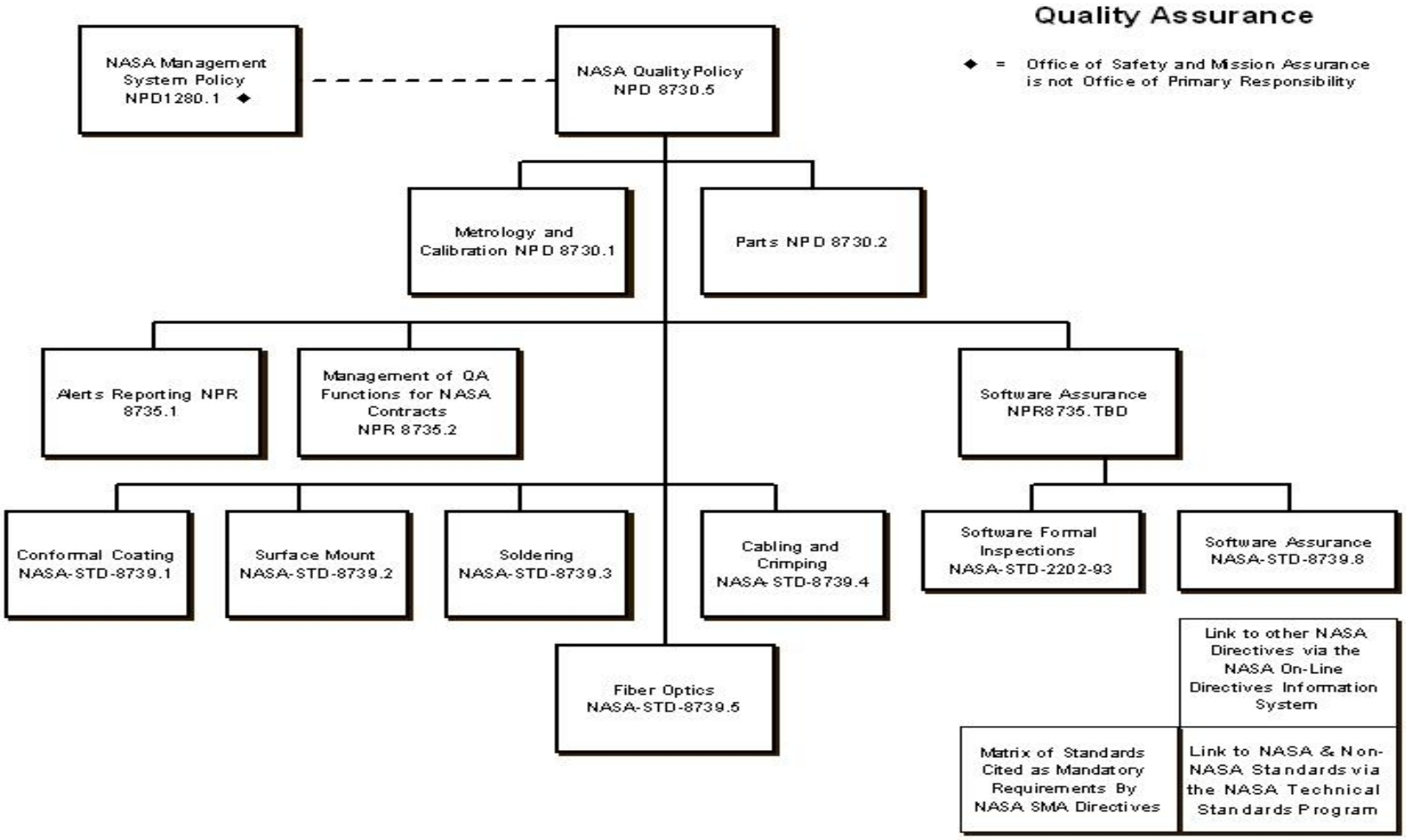
Safety and Mission Assurance Requirements



Safety and Mission Assurance Requirements



Safety and Mission Assurance Requirements



Requirements Management (Waivers/ Exceptions Approval/Acceptance)

- For technical and operational decisions dealing with residual human safety risk, where residual risk is defined as that added risk associated with operations outside of established design, safety or operational requirements (e.g. CILs, waivers, exceptions, non-compliances, "accepted risk" hazards, etc.):
  - The cognizant technical authority (Engineering, SMA, Medical) must formally approve based on the technical merit of the case;

  and,
  - The cognizant institutional Safety and Mission Assurance authority must approve based his/her independent judgment that the risk is acceptable;

  and,
  - The actual risk taker(s)* (or official spokesperson(s)) and his/her/their supervisory chain) must formally consent to taking the risk;

  and
  - The accountable* program, project or operations manager must formally accept the risk.

  *Note: when the people at risk are the general public, off of NASA property, the risk must be accepted by the Administrator